SMARTFILTER DA

SECURE COMPUTING

SmartFilter DA® Version 4.0.1

Release Notes

Welcome!

This document provides information about SmartFilter DA, version 4.0.1. In this document you'll find information and issues that you should consider before using SmartFilter DA. Please review its contents carefully.

Contents...

Welcome! 1
Change summary 2
Requirements 2
Installation and setup 4
Upgrading 7
General issues 9
Available hotfix 9
For additional information 10

Change summary

The following is a list of changes made to the 4.0.1 release of SmartFilter DA:

- Enhanced filtering engine performance for high traffic installations
- Improved overall block page performance
- Fixed issue where filter could be incorrectly forced into warn bypass mode
- Fixed issues with installation and upgrading of multi-server filter systems
- Fixed issue where errors would occur if duplicate URLs were added under custom exception categories
- Improved detection and handling of invalid custom allow/block list entries within the user interface

Requirements

SmartFilter DA works with Red Hat Linux 7.3, Enterprise Linux AS 3.0 Update 4, Enterprise Linux ES 3.0 Update 4, and Red Hat Enterprise Server 4.0 Update 2.

Before installing SmartFilter DA, check the Red Hat Web site to ensure that you've installed the latest security patches on your Red Hat system.

Hardware and OS requirements

The installation requirements for SmartFilter DA are:

- Pentium 750 MHz processor (1 GHz or higher recommended)
- One of the following operating systems:
  - Red Hat Linux 7.3
  - Enterprise Advanced Server 3.0
  - Enterprise Enterprise Server 3.0
  - Red Hat Enterprise Server 4.0

  Note: *Security-Enhanced Linux (SELinux) is not supported.*
- Each filter server must run the same operating system version

  Note: *SmartFilter DA requires the English version of the operating system.*
- 512 MB RAM (1 GB or higher recommended)
- 6 GB disk space free (on the partition that contains the */opt/n2h2 directory*)
- Network connection with Internet access (or connection to a proxy server with Internet access)

RPM requirements

SmartFilter DA requires certain RedHat Package Manager files (RPMs). If you install SmartFilter DA with Red Hat Linux 7.3, SmartFilter DA Setup can install these RPMs for you. If you install SmartFilter with Red Hat Enterprise Linux 3.0 or Red Hat Enterprise Server 4.0, you must install these RPMs yourself prior to running SmartFilter DA Setup. (For a list of the RPMs required for installation, see Appendix A in the *SmartFilter DA Installation Guide*.)

You can find the Enterprise Linux 3.0 and Red Hat Enterprise Server 4.0 RPMs on your Red Hat Installation CDs. Or, if you're a Red Hat Enterprise Linux subscriber, you can also access the RPMs on the Red Hat Network Web site. To access the RPMs from the Red Hat Network Web site, follow these steps:

1. Browse to *https://rhn.redhat.com/*.
2. Enter the user name and password provided with your Red Hat subscription.
3. Click the **Channels** tab.
4. In the **Channel** list, select the appropriate version of Red Hat.
5. Click the **Downloads** link.
6. Click the disk containing the required RPMs.

Installation and setup

To help ensure that Web filtering remains available when one machine is down, you can install multiple installations of SmartFilter DA. When installed in an array (or cluster), multiple installations of SmartFilter DA also let you implement load balancing to improve network performance during heavy traffic periods.

If you install SmartFilter DA on multiple machines, be sure that all machines are running with the same date/time and that the machines reside in the same local area network. To synchronize the machines' dates and times using the Network Time Protocol (NTP) daemon, go to *www.redhat.com/docs* and click the Customizations Guide listed under your version of Red Hat Linux.

Installing SmartFilter DA

Prior to installing SmartFilter DA, ensure that the machine you're installing it on has direct Internet access (or access to a proxy that can negotiate HTTP/HTTPS transactions). To install SmartFilter DA on a machine that connects through a firewall, you must first configure the firewall to allow inbound and outbound HTTPS access for this machine.

General installation steps

After you've ensured that all of the required RPMs are installed, you're ready to install SmartFilter DA.

1. Type `tar -zxvpf TarFileName.tgz` to extract the contents of the tar file. For `TarFileName`, type the name of the tar file you downloaded from Secure Computing.
2. Type `cd TarFileName` to change to the tar file directory.
3. With superuser privileges, type `./install`
   To exit the installation process at any time, press **CTRL+ C.**

Accessing the SmartFilter DA user interface

SmartFilter DA includes an easy-to-use Web-based interface that lets you customize filtering for your organization. You can open the Web-based interface using any machine on your network that has access to the machine you installed SmartFilter DA on.

To access the SmartFilter DA user interface

Note: *For optimal viewing, open the SmartFilter DA interface with Microsoft Internet Explorer 5.5 or later, or Mozilla 1.0 or later. You must enable JavaScript in your browser to take advantage of all SmartFilter DA features.*

1. Open a new browser window.
2. In the **Address** box or **Location** box, type **https://Address/controlcenter** For **Address**, type the IP address or fully qualified domain name (FQDN) of the machine where SmartFilter DA is installed.
3. In the **Look In** list, click **Local**.
4. Type the logon name and password you entered in the configuration wizard, and then click **OK**.

You can access the Control Center in the future using your network name and password. First click the Directory Services tab under Configure System to specify the directory service where your network name resides. Then click the Change Logon button under Change My Profile to select your network name as your new Control Center logon name.

Configuring SmartFilter DA

The first time you open the SmartFilter DA user interface, a configuration wizard appears. Follow the prompts in this wizard to specify key settings and register SmartFilter DA. To successfully register, you'll need your serial number (provided by Secure Computing). Keep your serial number handy after installation, as you will need it to reinstall SmartFilter DA or upgrade to a later version. If you do not have a serial number, contact your SmartFilter DA representative.

Immediately after configuration, SmartFilter DA downloads and processes the Web content information required for filtering. This initial process can take up to an hour, depending on the speed of your connection. During this time filtering is not available. To view the status of download processing, open the SmartFilter DA user interface, click the Configure System tab, and then click the Control List tab. (To view download processing as it occurs, click the Control List tab again to manually refresh the page.)

If download processing fails, it may be because registration was unsuccessful. To retry registration, open the configuration wizard using either of these methods:

- Click the Configure System tab, click the Advanced tab, and then click the Re-register button.
- In your browser's Address box or Location box, type **https://Address/n2h2configwizard**, where **Address** is the IP address or fully qualified domain name (FQDN) of the machine where SmartFilter is installed.

Note: *If you have multiple SmartFilter machines, be sure to re-run the configuration wizard on all machines.*

Installing SmartReporter

During installation of SmartFilter DA, you're prompted for the location of the database server. After you specify the machine's address, SmartFilter DA automatically creates the reporting database for you on that machine.

If reports are taking longer to view than expected, schedule the reports to be e-mailed to you once they're ready. For information on scheduling reports, see the *SmartFilter DA SmartReporter Administration Guide*. Alternatively, you can tune PostgreSQL settings to optimize performance. For information on tuning PostgreSQL, go to *www.securecomputing.com/pdf/sr_postgres_config.pdf*

Accessing the SmartReporter user interface

As with SmartFilter DA, you can easily access the SmartReporter Web-based interface using any machine on your network that has access to the machine you installed SmartFilter DA on.

To access the SmartReporter user interface

Note: *For optimal viewing, open the SmartReporter interface with Microsoft Internet Explorer 5.5 or later, or Mozilla 1.0 or later. You must enable JavaScript in your browser.*

1. Open a new browser window.
2. In the **Address** box or **Location** box, type **https://Address/smartreporter** For **Address**, type the IP address or fully qualified domain name (FQDN) of the machine where SmartFilter DA is installed.
3. In the **Look In** list, click **Local**.
4. Type your logon name and password, and then click **OK**. (The defaults are **admin**, **password**.)

To change your logon password, on the machine where you installed SmartFilter, open a command line and type:

```
/opt/n2h2/reports/bin/admin_util -u name -p password
```

where `name` is your current logon name and `password` is the new logon password

(For a list of all command line options related to SmartReporter logon accounts, type `admin_util -h`)

Upgrading

For upgrading SmartFilter DA 4.0 to SmartFilter DA 4.0.1, simply run the SmartFilter DA 4.0.1 installer and type **Yes** when prompted to upgrade.

Note: *When upgrading master/slave configurations, upgrade the master first.*

Use the following procedures to successfully upgrade from Sentian/Bess 2.5 to SmartFilter DA 4.0.1 with your filter settings intact:

Note: *Check Point FireWall-1 is not supported in SmartFilter DA.*

Procedure 1: Export your current filter settings

Before installing SmartFilter DA 4.x, export your current filter settings to a file. This precautionary step will let you roll back to a working installation of Filtering by N2H2 2.5 if necessary.

1. Open the Web user interface (**https://Address/controlcenter**).
2. On the navigation bar, click **Configure System**.
3. On the **Advanced** tab, click **Export**.
4. In the **Settings File** box, type a name for the export file.
5. Click **Export**.
6. The export file is automatically saved in the */opt/n2h2/export* directory. Copy this export file to a safe place.

Procedure 2: Run the export conversion script

Next run the export conversion script, *sf4_upgrade.pl*, on your Filtering by N2H2 2.5 machine. If you're upgrading your operating system, you **must** run this script to successfully preserve your settings. If you're keeping your existing operating system, it's still a good idea to run this script because it gives you a recourse in case you encounter problems later.

1. Extract the contents of the SmartFilter DA 4.x tar file you downloaded from Secure Computing.
2. Copy the script, *sf4_upgrade.pl*, to your Filtering by N2H2 2.5 machine.
3. With super user privileges, type `./sf4_upgrade.pl -o FileName,` where `FileName` is a descriptive name for the generated export file.
4. The export file is automatically saved in the current directory. Copy this export file to a safe place.

Note: *The export files you created in procedures 1 and 2 contain the same filter settings, but in different formats. The file from procedure 1 works with Filtering by N2H2 v2.5; the file from procedure 2 works with SmartFilter DA v4.x.*

Procedure 3: Install SmartFilter DA

If you're keeping your existing operating system, simply run the SmartFilter DA 4.x installer and type **Yes** when prompted to upgrade.

If you're upgrading your operating system, install the new system software first. Then run the SmartFilter DA 4.x installer.

Procedure 4: Register SmartFilter DA

After you install SmartFilter DA, run the configuration wizard to register SmartFilter DA.

If you kept your existing operating system, you're finished; SmartFilter DA automatically begins filtering your organization's Web access using your previous settings. (If you notice any problems with your filter settings, you can import the file you created in procedure 2 as described below.)

Procedure 5: Import the upgrade file *(OS upgrades)*

If you upgraded your operating system, import the file you created in procedure 2.

1. Copy the export file you created in procedure 2 to the */opt/n2h2/export* directory.
2. Open the Web user interface (**https://Address/controlcenter**).
3. On the navigation bar, click **Configure System**.
4. On the **Advanced** tab, click **Import**.
5. In the **Settings File** list, select the export file.
6. Click **Import**.

After the import process is complete, SmartFilter DA begins filtering your organization's Web access using your previous settings.

General issues

This section contains general issues you may encounter with SmartFilter DA software.

Filtering through a NAT device

If a NAT device (such as a firewall, gateway router, or proxy server) is installed between client computers and your IFP-enabled device (such as a Squid proxy or Cisco PIX), certain SmartFilter DA functionality may not work as expected (for example, user- and IP address-level filtering, authorized override, and Monitor with Warning). To take advantage of all of SmartFilter DA's features, install your IFP-enabled device between the NAT device and the client computers.

SmartFilter DA cron jobs

SmartFilter DA installs the following cron jobs:

- Daily backup of admin database
- syncdb (upstream directory service synchronizer)
- Daily list verifier/submittal system

Configuring an SSL proxy

If you are installing SmartFilter DA in a private network that does NOT have direct Internet access, and that has a proxy gateway that allows for outbound/inbound HTTP/HTTPS traffic, enter the address and port for your upstream proxy when prompted in the configuration wizard.

HTTPS and Squid

When browsing HTTPS blocked sites through a SmartFilter DA enabled Squid Proxy, the user will receive a Squid error page instead of the standard SmartFilter DA block page.

Available hotfix

There is a possibility that low level administrators could access the custom allow and block lists of the parent administrator. Hotfix 4.0.1.00.H01 is available to eliminate this possibility. To obtain this hotfix, browse to http://www.securecomputing.com/index.cfm?skey=1591.

For additional information

For more information on installing SmartFilter DA, or to learn about SmartFilter DA features and access step-by-step procedures, view the *SmartFilter DA Installation Guide*, *SmartFilter DA Administration Guide*, and *SmartFilter DA SmartReporter Administration Guide*. These documents are located on the Web at *www.securecomputing.com/goto/smartfilter/downloads*.

You can use the SmartFilterWhere tool to find out how specific sites are categorized by Secure Computing. The tool is available at *www.smartfilterwhere.com*.

You must have Acrobat Reader installed on your machine to view the guides; it is available for download from *www.adobe.com*.

SECURE COMPUTING CORPORATION

Technical Support Information
E-mail — support@securecomputing.com
Phone — +1.800.700.8328 or +1.651.628.1500
Web — www.securecomputing.com

Product names used within are trademarks of their respective companies.
Copyyright © 2006 Secure Computing Corporation. All rights reserved.